(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 October 2013 (24.10.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/158060 A1

(51) International Patent Classification:
H04W 12/08 (2009.01) *H04W 88/02* (2009.01)
H04W 12/06 (2009.01) *H04W 92/18* (2009.01)

(21) International Application Number:
PCT/US2012/033748

(22) International Filing Date:
16 April 2012 (16.04.2012)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95052 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **PHEGADE, Vinay** [US/US]; 16675 NW Avondale Dr., Beaverton, Oregon 97006 (US). **BAKSHI, Sanjay** [US/US]; 15222 NW Red Cedar Ct., Portland, Oregon 97231 (US).

(74) Agents: **AGHEVLI, Ramin** et al.; Caven & Aghevli, c/o CPA GLOBAL, P.O. Box 52050, Minneapolis, Minnesota 55402 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) **Title**: SCALABLE SECURE EXECUTION

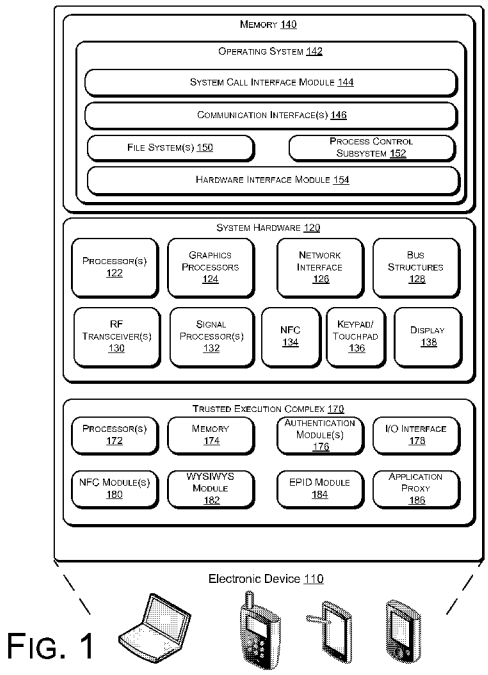

FIG. 1

(57) **Abstract**: In one embodiment a controller comprises logic configured to establish a pairing with a remote processor in a second electronic device, create a first secure communication channel with the remote processor, transmit a first portion of a processing task to the remote processor via the first secure channel, receive, via a second communication channel, an input from the first portion of the processing task, and complete at least a second portion of the processing task using the input. Other embodiments may be described.

WO 2013/158060 A1

SCALABLE SECURE EXECUTION

BACKGROUND

The subject matter described herein relates generally to the field of computing and more particularly to systems and methods which allows an electronic devices to utilize processing capacity in a remote electronic device.

In a typical electronic commerce transaction the merchant (and underlying ecosystem), is not certain that the individual conducting the transaction is the authorized person. When fraudulent transactions are accepted by the online ecosystem there is an underlying fraud cost that is generally borne by the relying party, in this example the merchant, or by the defrauded individual.

Another weakness in the online space is the ever-present threat of system malware, which is often used to steal personal information, including payment credentials, for use by unauthorized individuals. This threat has an effect on a certain percentage of the population who will not conduct online activity due to fear of having their information compromised. This reduces efficiencies that can be gained through online commerce and limits the amount of goods and services purchased by concerned individuals, limiting the growth of online commerce.

Some computing systems may utilize a secure controller, separate from the main processor, encased in a trusted execution complex to manage authentication processes. Secure controllers may have limited computational and memory resources, such that computationally expensive tasks may be challenging for secure controllers to implement.

Accordingly systems and techniques to provide secure execution to enable computationally expensive tasks to be offloaded to a remote processor may find utility.

BRIEF DESCRIPTION OF THE DRAWINGS

The detailed description is described with reference to the accompanying figures.

Fig. 1 is a schematic illustration of an exemplary electronic device which may be adapted to include infrastructure to implement scalable secure execution in accordance with some embodiments.

Fig. 2 is a high-level schematic illustration of an exemplary network architecture for scalable secure execution in accordance with some embodiments.

Fig. 3 is a schematic illustration of an exemplary architecture for scalable secure execution in accordance with some embodiments.

Fig. 4 is a flowchart illustrating operations in a method to implement scalable secure execution in accordance with some embodiments.

Fig. 5 is a schematic illustration of an exemplary system for scalable secure execution, in accordance with some embodiments.

DETAILED DESCRIPTION

Described herein are exemplary systems and methods to implement scalable secure execution in electronic devices. Some embodiments of the systems and methods described herein may find utility in the context of network security, and particularly in electronic commerce settings. Some embodiments described herein may enable a trusted execution engine, also sometimes referred to as a secure processor or a manageability engine, to offload one or more portions of a processing task to a remote processor which may be located on a separate processing device. By way of example, in the context of a electronic commerce application a trusted execution engine in a first computing device may offload graphics-intensive operations such as bitmap generation to a remote processor located on a separate computing device. The remote processor may forward the bitmap to an application executing on the untrusted execution complex of the first device, which may present the bitmap on a display and collect input from the display. Offloading the bitmap generation to a remote processor inhibits malware on the first device from interfering with or snooping user inputs or outputs from the bitmap region.

This document provides description of hardware and software environments in which scalable secure execution may be implemented and of exemplary operations to implement scalable secure execution. In the following description, numerous specific details are set forth to provide a thorough understanding of various embodiments. However, it will be understood by those skilled in the art that the various embodiments may be practiced without the specific details. In other instances, well-known methods, procedures, components, and circuits have not been illustrated or described in detail so as not to obscure the particular embodiments.

Fig. 1 is a schematic illustration of an exemplary electronic device 110 which may be adapted to implement scalable secure execution in accordance with some embodiments. As illustrated in Fig. 1, electronic device 110 may be embodied as a conventional mobile device such as a mobile phone, tablet computer portable computer, or personal digital assistant (PDA).

In some embodiments an electronic device may include a trusted execution complex, which may also be referred to as a trusted execution engine or sometimes as a secure element or a manageability engine. The trusted execution complex may comprise one or more controllers that are separate from the primary execution complex, sometimes referred to as an untrusted execution complex. The separation may be physical in the sense that the trusted execution complex may be physically separate from the untrusted execution complex. Alternatively, the trusted execution complex may logical in the sense that the trusted execution complex may be

hosted on same chip or chipset that hosts the untrusted execution complex, but separated at the silicon level such that the trusted execution complex is secure.

In various embodiments, electronic device 110 may include or be coupled to one or more accompanying input/output devices including a display, one or more speakers, a keyboard, one or more other I/O device(s), a mouse, or the like. Exemplary I/O device(s) may include a touch screen, a voice-activated input device, a track ball, a geolocation device, an accelerometer/gyroscope, biometric feature input devices, and any other device that allows the electronic device 110 to receive input from a user.

The electronic device 110 includes system hardware 120 and memory 140, which may be implemented as random access memory and/or read-only memory. A file store may be communicatively coupled to computing device 110. The file store may be internal to computing device 110 such as, *e.g.*, eMMC, SSD, one or more hard drives, or other types of storage devices. File store 180 may also be external to computer 110 such as, *e.g.*, one or more external hard drives, network attached storage, or a separate storage network.

System hardware 120 may include one or more processors 122, graphics processors 124, network interfaces 126, and bus structures 128. In one embodiment, processor 122 may be embodied as an Intel® Atom™ processors, Intel® Atom™ based System-on-a-Chip (SOC) or Intel ® Core2 Duo® processor available from Intel Corporation, Santa Clara, California, USA. As used herein, the term "processor" means any type of computational element, such as but not limited to, a microprocessor, a microcontroller, a complex instruction set computing (CISC) microprocessor, a reduced instruction set (RISC) microprocessor, a very long instruction word (VLIW) microprocessor, or any other type of processor or processing circuit.

Graphics processor(s) 124 may function as adjunct processor that manages graphics and/or video operations. Graphics processor(s) 124 may be integrated onto the motherboard of electronic device 110 or may be coupled via an expansion slot on the motherboard.

In one embodiment, network interface 126 could be a wired interface such as an Ethernet interface (see, e.g., Institute of Electrical and Electronics Engineers/IEEE 802.3-2002) or a wireless interface such as an IEEE 802.11a, b or g-compliant interface (see, e.g., IEEE Standard for IT-Telecommunications and information exchange between systems LAN/MAN--Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, 802.11G-2003). Another example of a wireless interface would be a general packet radio service (GPRS) interface (see, e.g., Guidelines on GPRS Handset Requirements, Global System for Mobile Communications/GSM Association, Ver. 3.0.1, December 2002).

Bus structures 128 connect various components of system hardware 128. In one embodiment, bus structures 128 may be one or more of several types of bus structure(s) including a memory bus, a peripheral bus or external bus, and/or a local bus using any variety of available bus architectures including, but not limited to, 11-bit bus, Industrial Standard Architecture (ISA), Micro-Channel Architecture (MSA), Extended ISA (EISA), Intelligent Drive Electronics (IDE), VESA Local Bus (VLB), Peripheral Component Interconnect (PCI), Universal Serial Bus (USB), Advanced Graphics Port (AGP), Personal Computer Memory Card International Association bus (PCMCIA), and Small Computer Systems Interface (SCSI), a High Speed Synchronous Serial Interface (HSI), a Serial Low-power Inter-chip Media Bus (SLIMbus®), or the like.

Electronic device 110 may include an RF transceiver 130 to transceive RF signals, a Near Field Communication (NFC) radio 134, and a signal processing module 132 to process signals received by RF transceiver 130. RF transceiver may implement a local wireless connection via a protocol such as, e.g., Bluetooth or 802.11X. IEEE 802.11a, b or g-compliant interface (see, e.g., IEEE Standard for IT-Telecommunications and information exchange between systems LAN/MAN--Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, 802.11G-2003). Another example of a wireless interface would be a WCDMA, LTE, general packet radio service (GPRS) interface (see, e.g., Guidelines on GPRS Handset Requirements, Global System for Mobile Communications/GSM Association, Ver. 3.0.1, December 2002).

Electronic device 110 may further include one or more input/output interfaces such as, e.g., a keypad 136 and a display 138. In some embodiments electronic device 110 may not have a keypad and use the touch panel for input.

Memory 140 may include an operating system 142 for managing operations of computing device 110. In one embodiment, operating system 142 includes a hardware interface module 154 that provides an interface to system hardware 120. In addition, operating system 140 may include a file system 150 that manages files used in the operation of computing device 110 and a process control subsystem 152 that manages processes executing on computing device 110.

Operating system 142 may include (or manage) one or more communication interfaces 146 that may operate in conjunction with system hardware 120 to transceive data packets and/or data streams from a remote source. Operating system 142 may further include a system call interface module 144 that provides an interface between the operating system 142 and one or more application modules resident in memory 130. Operating system 142 may be embodied as a

UNIX operating system or any derivative thereof (*e.g.*, Linux, Android, *etc.*) or as a Windows® brand operating system, or other operating systems.

Electronic device 110 may comprise a trusted execution engine 170. In some embodiments the trusted execution engine 170 may be implemented as an independent integrated circuit located on the motherboard of the electronic device 110, while in other embodiments the trusted execution engine 170 may implemented as a dedicated processor block on the same SOC die, while in other embodiments the trusted execution engine may be implemented on a portion of the processor(s) 122 that is segregated from the rest of the processor(s) using HW enforced mechanisms

In the embodiment depicted in Fig. 1 the trusted execution engine 170 comprises a processor 172, a memory module 174, one or more authentication module(s) 176, and an I/O module 178, a near field communication (NFC) module, a what you see is what you sign (WYSIWYS) module 182, an enhanced privacy identification (EPID) module 184 and one or more application proxies 186. In some embodiments the memory module 174 may comprise a persistent flash memory module and the various functional modules may be implemented as logic instructions encoded in the persistent memory module, e.g., firmware or software. The I/O module 178 may comprise a serial I/O module or a parallel I/O module. Because the trusted execution engine 170 is separate from the main processor(s) 122 and operating system 142, the trusted execution engine 170 may be made secure, i.e., inaccessible to hackers who typically mount SW attacks from the host processor 122.

In some embodiments the trusted execution engine may define a trusted execution complex in a host electronic device in which scalable secure execution procedures may be implemented to allow portions of a processing task to be offloaded to a remote processor on a different electronic device. Offloading the processing onto a remote processor inhibits the ability of malware or snooping software executing on the untrusted execution complex to tamper with or read inputs, outputs, or processing results form operations.

Fig. 2 is a high-level schematic illustration of a network environment in which scalable secure execution procedures may be implemented. Referring to Fig. 2, an electronic device 110 and a remote device 112 may be coupled to one or more remote servers 230 via a network 240. Electronic device 110 may comprise a near field communication (NFC) interface to enable wireless communication with remote device 112 via a suitable near field communication link. In some embodiments each of electronic device 110 and remote device 112 may be embodied as a mobile telephone, tablet, PDA or other mobile computing device as described with reference to electronic device 110, above. Network 240 may be embodied as a public communication

network such as, e.g., the internet, or as a private communication network, or combinations thereof.

Remote server(s) 230 may be embodied as computer systems. In some embodiments the server(s) 230 may be embodied as an electronic commerce server and may be managed by a vendor or by a third party which operates a secure platform. Other remote server(s) 230 may be operated by a vendor or by a third-party payment system, e.g., a transaction clearing service or a credit card service.

Fig. 3 is a more detailed, schematic illustration of a system to implement scalable secure execution according to some embodiments. Referring to Fig. 3, the electronic device 110 may be coupled to a transaction system 350 via network 340. In addition, the electronic device 110 may be coupled to a validation system 360, which may be separate from or integrated with transaction system 350. Similarly, in some embodiments the remote device 112 may also be coupled to a transaction system 350 and validation system 360 via network 340.

In some embodiments a browser or other application 320 may execute in the untrusted execution complex of electronic device 110. Browser 320 may include an authentication plugin 322 which cooperates with authentication module 176 that executes on the trusted execution complex of electronic device 110. Remote device 112 includes an input output module 336, a processor 334, and an authentication module 322 residing in memory 330.

Remote entities that manage transactions, identified as a transaction system 350 in Fig. 2, may be embodied as electronic commerce websites or the like and may be coupled to the host device via a communication network 340. In use, an owner or operator of electronic device 110 may access the transaction system 350 using a browser 320 or other application software via the network to initiate an electronic commerce transaction on the system 350.

The authentication module 176, alone or in combination with an authentication plug-in 322, the input/output module 178 and the secure sprite generator 179, and the processor 334 and authentication module 332 on remote device 112 may implement scalable secure execution operations in which portions of a processing task implemented by the processor 172 are offloaded to remote processor 334 of remote device 112.

Having described various structures of a system to implement scalable secure execution, operating aspects of a system will be explained with reference to Fig. 4. In some embodiments the operations depicted in the flowchart of Fig. 4 may be implemented by processor 172 of the trusted execution engine 170, alone or in combination with the processor 122 on that executes in the untrusted execution complex of electronic device and the processor 334 of remote device 112.

Referring to Fig. 4, in some embodiments the operations depicted in Fig. 4 at operations 405 and 410 a secure pairing is established between the trusted execution engine, also referred to as the secure controller, and the remote processor, e.g., the processor 334 on remote device 112. In some embodiments the pairing may be initiated by a user initiating a registration sequence, e.g., by tapping remote device 112 on the electronic device 110 or otherwise launching a registration process. In response to the registration request the processor 172 of the trusted execution engine 170 launches the authentication module 176 and the processor 334 of remote device 112 launches the authentication module 332. The respective authentication modules 322, 332 may develop a shared secret using a suitable cryptographic algorithm, e.g., a Diffie-Hellman key exchange protocol or the like.

At operations 415 and 420 the trusted execution engine 170 and the remote processor 334 establish a secure communication connection by way of their respective input/output module 178, 336. The communication connection may be implemented via a wireless connection or any other suitable communication medium, e.g., an infrared connection or a wired network connection.

At operation 425 a browser 320 or other suitable application is launched on the local processor 122 of the electronic device 110. At operations 430 and 435 a discovery process is implemented between the electronic device 110 and the remote device 112. By way of example, in some embodiments the devices 110, 112 may comprise a Bluetooth or other wireless networking capability and may discover one another via the wireless network.

At operation 440 the application on the browser connects to a remot server. By way of example, in the embodiment depicted in Fig. 3 the browser may be used to connect to a transaction system 350, which may be an electronic commerce web site or the like. In some embodiments the electronic device 110 receives a login request from the remote server, and in response the authentication plugin 322 which executes in the untrusted execution complex invokes the authentication module 176 in the trusted execution complex.

In some embodiments the trusted execution complex may generate a bitmap image for a login screen and present it on the display 138 of the electronic device. By way of example, in some embodiments the WYSIWYS module 182 opens a secure window on a display of electronic device and presents an authorization request in a dialog box 380 on the window. A user of the electronic device 110 responds to the authorization request by entering an input in the secure window, which authorizes the login request. The WYSIWYS module 182 may generate a pin which is associated with the input.

However, in some embodiments the trusted execution complex offloads the process of generating a bitmap to the processor 334 on the remote device 112. In such embodiments the authentication module 176 executing on processor 172 generates a confirmation code and forwards the confirmation code and a confirmation page to processor 334 on the remote device 112.

At operation 450 the processor 334 on remote device 112 receives the confirmation code, and at operation 455 the processor 334 composes the bitmap and encrypts the bitmap using the shared secret. In addition, the processor 334 on remote device 112 generates coordinates for user input elements such as a username and password combination.

The bitmap is passed back to the electronic device 110. In some embodiments the secure sprite generator 179 may render the bitmap on the display 138. In other embodiments the graphics processor(s) 124 in the untrusted execution complex may render the bitmap on display 138. Referring briefly to Fig. 3, the rendered bitmap pay present a dialog box 380 on the display. Dialog box 380 may comprise an input window 382 for a username, an input window 384 for a password, and an input mechanism such as a keyboard 386 for the user to enter inputs in the dialog box 380.

A user may enter a username/password combination in the respective windows 382, 384 using the keyboard 386. At operation 475 the inputs are received in the secure controller. In some embodiments the trusted execution engine blocks the bitmap region from the system hardware such that inputs into the dialog box 380 are not visible to the untrusted execution complex. In such embodiments the inputs may be detected directly by input/output interface 178. In other embodiments the inputs may be detected by the inputs may be captured by the authentication plug-in 322 executing in the untrusted execution complex. In such embodiments it should be noted that sniffing by malware is inhibited because the input coordinates were generated on processor 334 of remote device 112. Thus, malware would lack knowledge of the input coordinates or the inputs associated with the coordinates.

At operation 480 the user inputs are validated. By way of example, in some embodiments the authentication module 176 invokes the EPID module 184, which generates and wraps an identification packet and applies a signature that attests that the packet was obtained securely over the NFC communication link and that the WYS pin was obtained securely using the WYSIWYS module 182. The electronic device 110 forwards the wrapped identification packet to a remote validation server 460, which validates the user input and returns an authorization response to the electronic device 110. In some embodiments the validation response is received

via the I/O interface 178 in the trusted execution engine 170 and is therefore not accessible to the untrusted operating environment of the electronic device 110.

At operation 485 the authentication module 176 reviews the response from the remote validation server 460. If, at operation 485, the response from the remote authentication server 430 indicates that the login is not authorized then control passes to operation 490 and the login procedure is terminated and access denied. By contrast, if at operation 485 the response from the remote authentication server 430 indicates that the login is authorized then control passes to operation 495 and a secure communication session may be initiated between the electronic device 110 and the transaction system 350.

As described above, in some embodiments the electronic device 110 may be embodied as a computer system. Fig. 5 is a schematic illustration of a computer system 500 in accordance with some embodiments. The computer system 500 includes a computing device 502 and a power adapter 504 (e.g., to supply electrical power to the computing device 502). The computing device 502 may be any suitable computing device such as a laptop (or notebook) computer, a personal digital assistant, a desktop computing device (e.g., a workstation or a desktop computer), a rack-mounted computing device, and the like.

Electrical power may be provided to various components of the computing device 502 (e.g., through a computing device power supply 506) from one or more of the following sources: one or more battery packs, an alternating current (AC) outlet (e.g., through a transformer and/or adaptor such as a power adapter 504), automotive power supplies, airplane power supplies, and the like. In some embodiments, the power adapter 504 may transform the power supply source output (e.g., the AC outlet voltage of about 110VAC to 240VAC) to a direct current (DC) voltage ranging between about 5VDC to 12.6VDC. Accordingly, the power adapter 504 may be an AC/DC adapter.

The computing device 502 may also include one or more central processing unit(s) (CPUs) 508. In some embodiments, the CPU 508 may be one or more processors in the Pentium® family of processors including the Pentium® II processor family, Pentium® III processors, Pentium® IV , or CORE2 Duo processors available from Intel® Corporation of Santa Clara, California. Alternatively, other CPUs may be used, such as Intel's Itanium®, XEON , and Celeron® processors. Also, one or more processors from other manufactures may be utilized. Moreover, the processors may have a single or multi core design.

A chipset 512 may be coupled to, or integrated with, CPU 508. The chipset 512 may include a memory control hub (MCH) 514. The MCH 514 may include a memory controller 516 that is coupled to a main system memory 518. The main system memory 518 stores data and

sequences of instructions that are executed by the CPU 508, or any other device included in the system 500. In some embodiments, the main system memory 518 includes random access memory (RAM); however, the main system memory 518 may be implemented using other memory types such as dynamic RAM (DRAM), synchronous DRAM (SDRAM), and the like. Additional devices may also be coupled to the bus 510, such as multiple CPUs and/or multiple system memories.

The MCH 514 may also include a graphics interface 520 coupled to a graphics accelerator 522. In some embodiments, the graphics interface 520 is coupled to the graphics accelerator 522 via an accelerated graphics port (AGP). In some embodiments, a display (such as a flat panel display) 540 may be coupled to the graphics interface 520 through, for example, a signal converter that translates a digital representation of an image stored in a storage device such as video memory or system memory into display signals that are interpreted and displayed by the display. The display 540 signals produced by the display device may pass through various control devices before being interpreted by and subsequently displayed on the display.

A hub interface 524 couples the MCH 514 to an platform control hub (PCH) 526. The PCH 526 provides an interface to input/output (I/O) devices coupled to the computer system 500. The PCH 526 may be coupled to a peripheral component interconnect (PCI) bus. Hence, the PCH 526 includes a PCI bridge 528 that provides an interface to a PCI bus 530. The PCI bridge 528 provides a data path between the CPU 508 and peripheral devices. Additionally, other types of I/O interconnect topologies may be utilized such as the PCI Express architecture, available through Intel® Corporation of Santa Clara, California.

The PCI bus 530 may be coupled to an audio device 532 and one or more disk drive(s) 534. Other devices may be coupled to the PCI bus 530. In addition, the CPU 508 and the MCH 514 may be combined to form a single chip. Furthermore, the graphics accelerator 522 may be included within the MCH 514 in other embodiments.

Additionally, other peripherals coupled to the PCH 526 may include, in various embodiments, integrated drive electronics (IDE) or small computer system interface (SCSI) hard drive(s), universal serial bus (USB) port(s), a keyboard, a mouse, parallel port(s), serial port(s), floppy disk drive(s), digital output support (e.g., digital video interface (DVI)), and the like. Hence, the computing device 502 may include volatile and/or nonvolatile memory.

Thus, there is described herein an architecture and associated methods to implement scalable secure execution in electronic devices. In some embodiments the architecture uses hardware capabilities embedded in remote electronic device platform to perform computationally expensive processing tasks for a secure controller in a separate device. The execution complex

may be implemented in a trusted execution engine such that operations are not accessible to malware on an electronic device. In some embodiments the trusted execution engine may be implemented in a remote or attachable device, e.g., a dongle,

The terms "logic instructions" as referred to herein relates to expressions which may be understood by one or more machines for performing one or more logical operations. For example, logic instructions may comprise instructions which are interpretable by a processor compiler for executing one or more operations on one or more data objects. However, this is merely an example of machine-readable instructions and embodiments are not limited in this respect.

The terms "computer readable medium" as referred to herein relates to media capable of maintaining expressions which are perceivable by one or more machines. For example, a computer readable medium may comprise one or more storage devices for storing computer readable instructions or data. Such storage devices may comprise storage media such as, for example, optical, magnetic or semiconductor storage media. However, this is merely an example of a computer readable medium and embodiments are not limited in this respect.

The term "logic" as referred to herein relates to structure for performing one or more logical operations. For example, logic may comprise circuitry which provides one or more output signals based upon one or more input signals. Such circuitry may comprise a finite state machine which receives a digital input and provides a digital output, or circuitry which provides one or more analog output signals in response to one or more analog input signals. Such circuitry may be provided in an application specific integrated circuit (ASIC) or field programmable gate array (FPGA). Also, logic may comprise machine-readable instructions stored in a memory in combination with processing circuitry to execute such machine-readable instructions. However, these are merely examples of structures which may provide logic and embodiments are not limited in this respect.

Some of the methods described herein may be embodied as logic instructions on a computer-readable medium. When executed on a processor, the logic instructions cause a processor to be programmed as a special-purpose machine that implements the described methods. The processor, when configured by the logic instructions to execute the methods described herein, constitutes structure for performing the described methods. Alternatively, the methods described herein may be reduced to logic on, e.g., a field programmable gate array (FPGA), an application specific integrated circuit (ASIC) or the like.

In the description and claims, the terms coupled and connected, along with their derivatives, may be used. In particular embodiments, connected may be used to indicate that two

or more elements are in direct physical or electrical contact with each other. Coupled may mean that two or more elements are in direct physical or electrical contact. However, coupled may also mean that two or more elements may not be in direct contact with each other, but yet may still cooperate or interact with each other.

Reference in the specification to "one embodiment" or "some embodiments" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least an implementation. The appearances of the phrase "in one embodiment" in various places in the specification may or may not be all referring to the same embodiment.

Although embodiments have been described in language specific to structural features and/or methodological acts, it is to be understood that claimed subject matter may not be limited to the specific features or acts described. Rather, the specific features and acts are disclosed as sample forms of implementing the claimed subject matter.

CLAIMS

What is claimed is:

1. A controller for a first electronic device comprising:

logic configured to:

establish a pairing with a remote processor in a second electronic device;

create a first secure communication channel with the remote processor;

transmit a first portion of a processing task to the remote processor via the first secure channel;

receive, via a second communication channel, an input from the first portion of the processing task; and

complete at least a second portion of the processing task using the input.

2. The controller of claim 1, wherein the logic comprises a near field wireless communication interface to communicate with the remote processor.

3. The controller of claim 1, further comprising logic configured to add a confirmation code to the first portion of the processing task.

4. The controller of claim 1, further comprising a local processor coupled to the controller, and wherein the local processor comprises logic configured to:

receive, from the remote processor, an output of the first portion of the processing task; and

present the output on a display coupled to the local controller.

5. The controller of claim 4, wherein the local processor further comprises logic configured to:

receive an input from an input device; and

pass the input to the controller.

6. The controller of claim 4, further comprising logic configured to:

render a bitmap received from the remote processor; and

receive an input in the bitmap.

7. The controller of claim 6, further comprising logic configured to validate the input.

8. An electronic device, comprising:

a processor which is to implement an untrusted computing environment; and

a controller, comprising:

logic configured to:

logic configured to:

establish a pairing with a remote processor in a second electronic

device;

create a first secure communication channel with the remote processor;

transmit a first portion of a processing task to the remote processor via the first secure channel;

receive, via a second communication channel, an input from the first portion of the processing task; and

complete at least a second portion of the processing task using the input.

9. The electronic device of claim 8, wherein the logic comprises a near field wireless communication interface to communicate with the remote processor.

10. The electronic device of claim 8, further comprising logic configured to add a confirmation code to the first portion of the processing task.

11. The electronic device of claim 10, further comprising a local processor coupled to the controller, and wherein the local processor comprises logic configured to:

receive, from the remote processor, an output of the first portion of the processing task; and

present the output on a display coupled to the local controller.

12. The electronic device of claim 11, wherein the local processor further comprises logic configured to:

receive an input from an input device; and

pass the input to the controller.

13. The electronic device of claim 11, further comprising logic configured to:

render a bitmap received from the remote processor; and

receive an input in the bitmap.

14. The electronic device of claim 13, further comprising logic configured to validate the input.

15. A method, comprising:

establishing a pairing between a controller in a first electronic device and a remote processor in a second electronic device;

creating a first communication channel between the controller and the remote processor;

transmitting a first portion of a processing task from the controller to the remote processor via the first secure channel;

receiving in the controller, via a second communication channel, an input from the first portion of the processing task; and

completing, in the controller, at least a second portion of the processing task using the input.

16. The method of claim 15, further comprising adding a confirmation code to the first portion of the processing task.

17. The method of claim 16, further comprising:

receiving in a local processor an output from the remote processor of the first portion of the processing task; and

presenting the output on a display module coupled to the local processor.

18. The method of claim 17, further comprising:

receiving, in the local processor, an input from an input device; and

passing the input from the local processor to the controller.

19. The method of claim 15, further comprising validating the input.

20. A computer program product comprising logic instructions stored on non-transitory computer readable medium which, when executed by a controller, configure the controller to:

establish a pairing with a remote processor in a second electronic device;

create a first secure communication channel with the remote processor;

transmit a first portion of a processing task to the remote processor via the first secure channel;

receive, via a second communication channel, an input from the first portion of the processing task; and

complete at least a second portion of the processing task using the input.

21. The computer program product of claim 20, wherein the logic comprises a near field wireless communication interface to communicate with the remote processor.

22. The computer program product of claim 21, further comprising logic to add a confirmation code to the first portion of the processing task.

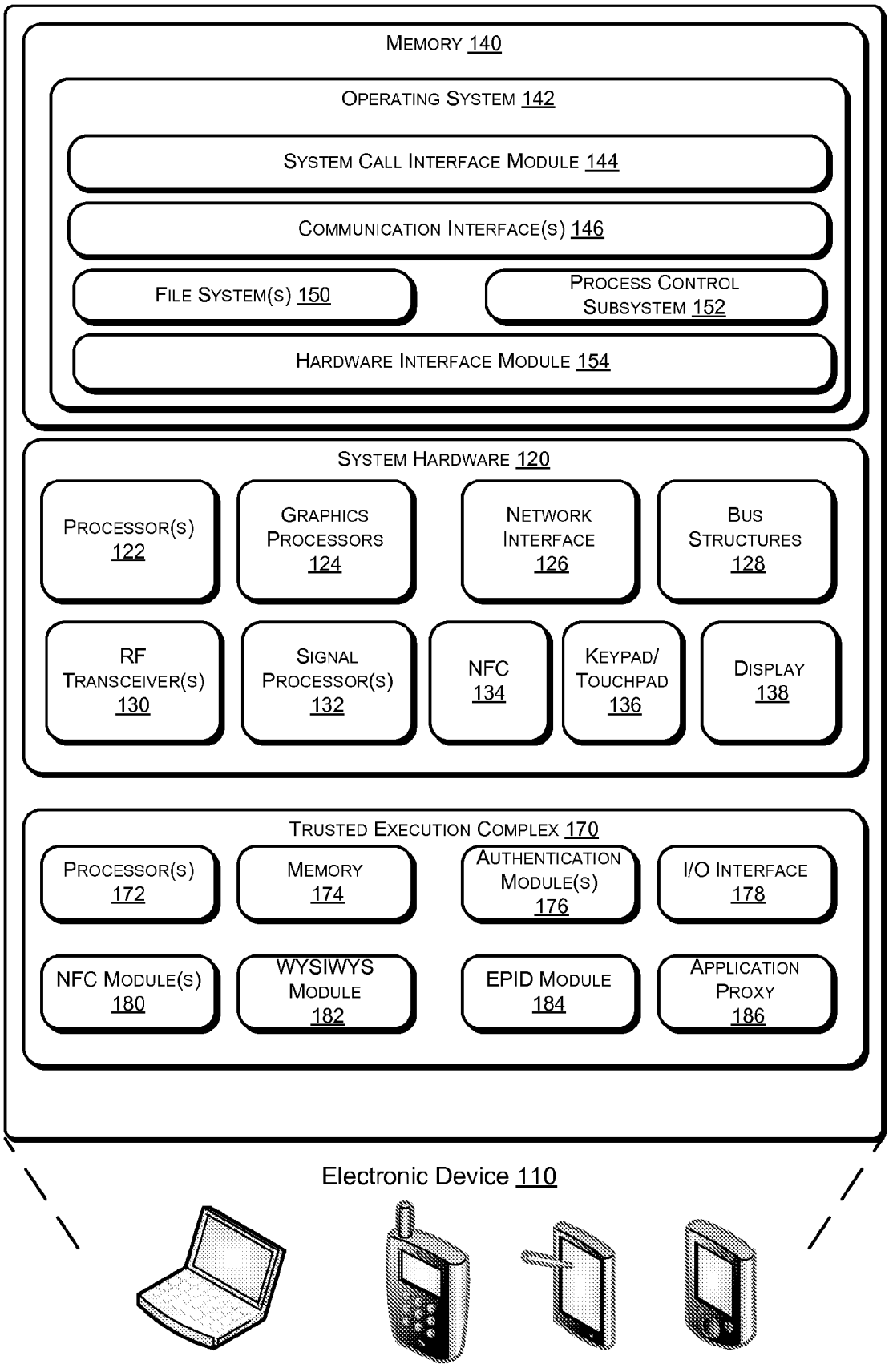
Memory 140
Operating System 142
System Call Interface Module 144
Communication Interface(s) 146
File System(s) 150
Process Control Subsystem 152
Hardware Interface Module 154
System Hardware 120
Processor(s) 122
Graphics Processors 124
Network Interface 126
Bus Structures 128
RF Transceiver(s) 130
Signal Processor(s) 132
NFC 134
Keypad/ Touchpad 136
Display 138
Trusted Execution Complex 170
Processor(s) 172
Memory 174
Authentication Module(s) 176
I/O Interface 178
NFC Module(s) 180
WYSIWYS Module 182
EPID Module 184
Application Proxy 186
Electronic Device 110

FIG. 1

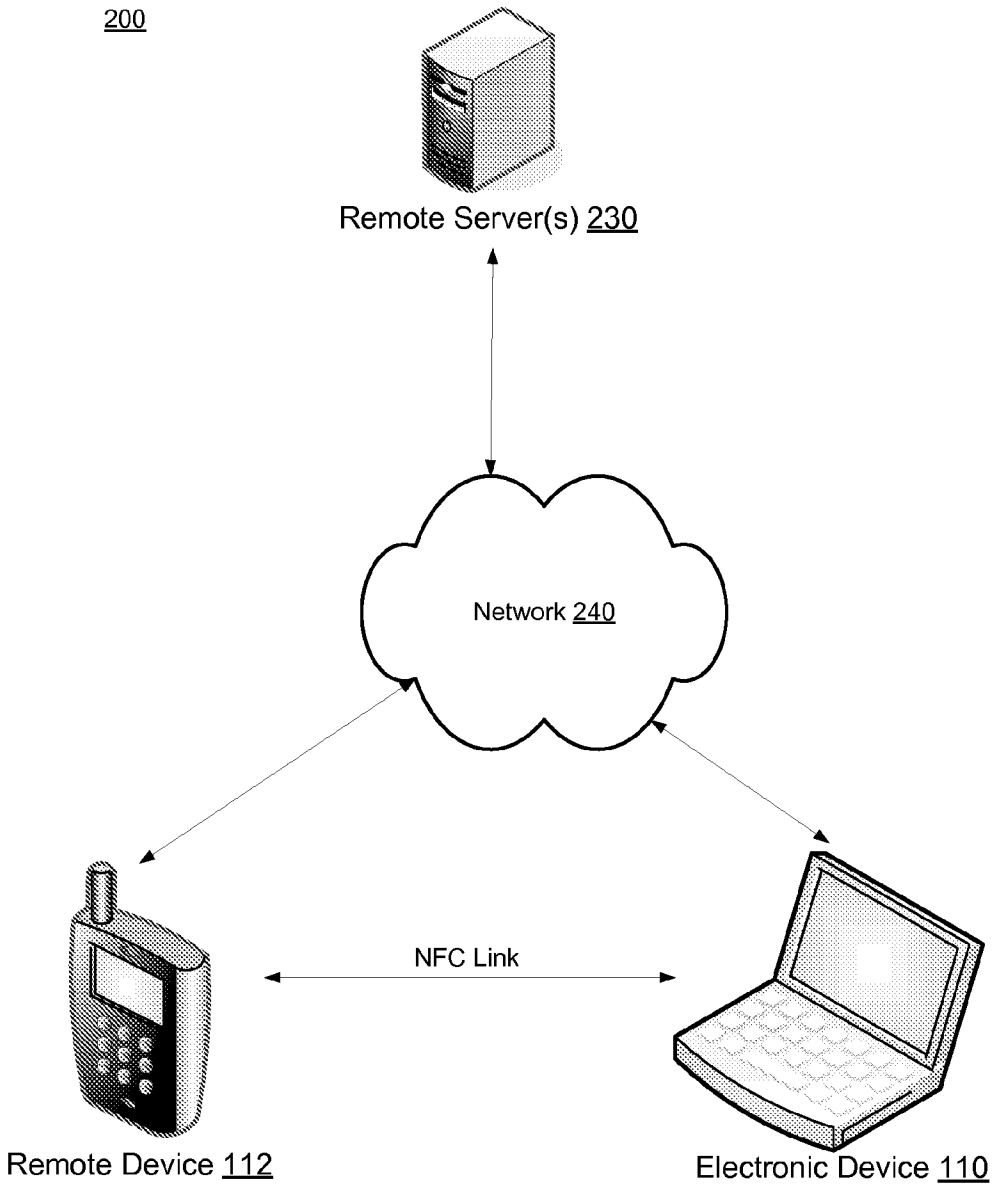
200
Remote Server(s) 230
Network 240
NFC Link
Remote Device 112
Electronic Device 110

FIG. 2

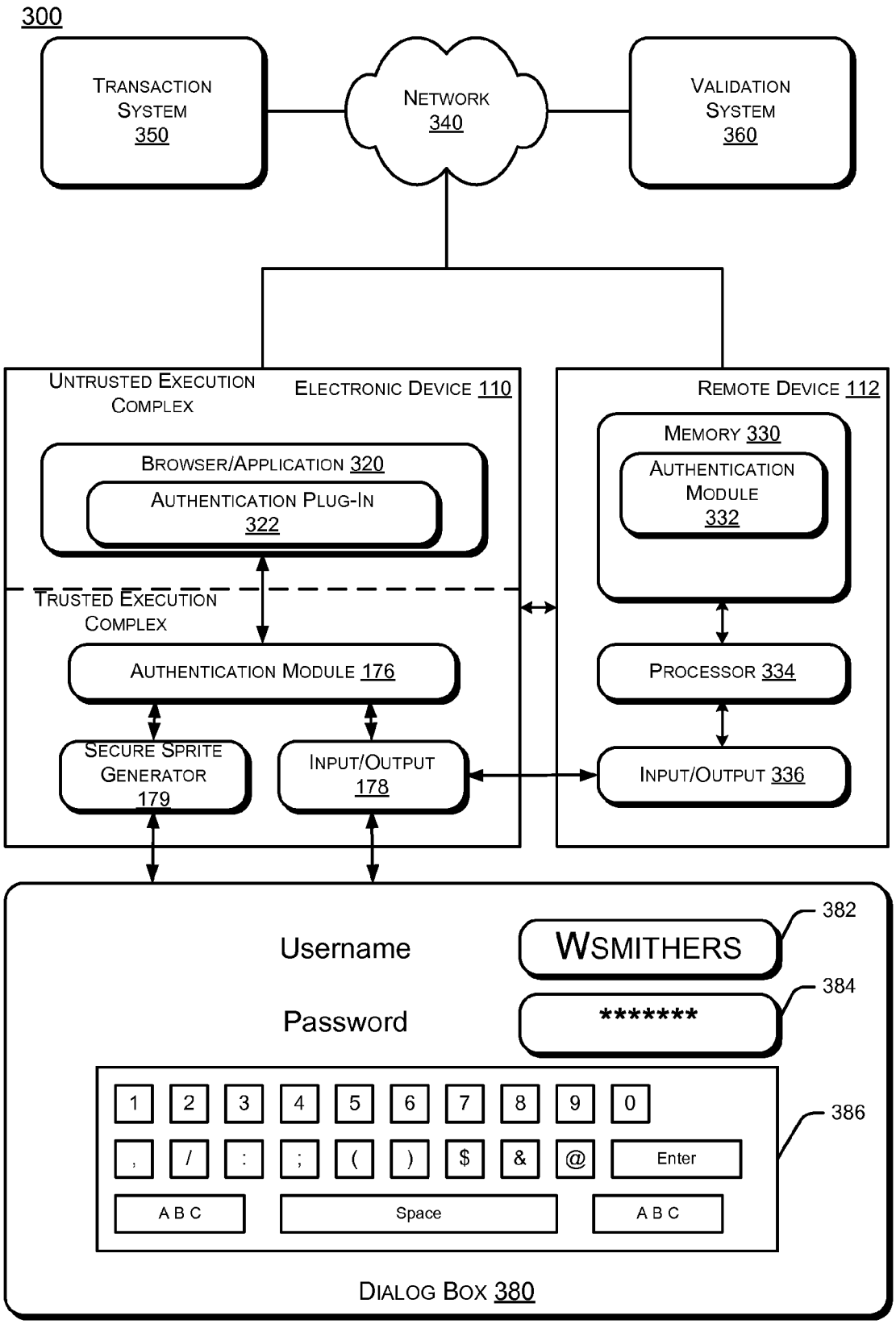
300
TRANSACTION SYSTEM 350
NETWORK 340
VALIDATION SYSTEM 360
UNTRUSTED EXECUTION COMPLEX
ELECTRONIC DEVICE 110
REMOTE DEVICE 112
BROWSER/APPLICATION 320
AUTHENTICATION PLUG-IN 322
MEMORY 330
AUTHENTICATION MODULE 332
TRUSTED EXECUTION COMPLEX
AUTHENTICATION MODULE 176
PROCESSOR 334
SECURE SPRITE GENERATOR 179
INPUT/OUTPUT 178
INPUT/OUTPUT 336
Username
WSMITHERS
382
Password
****
384
1 2 3 4 5 6 7 8 9 0
, / : ; ( ) $ & @ Enter
A B C
Space
A B C
386
DIALOG BOX 380

FIG. 3

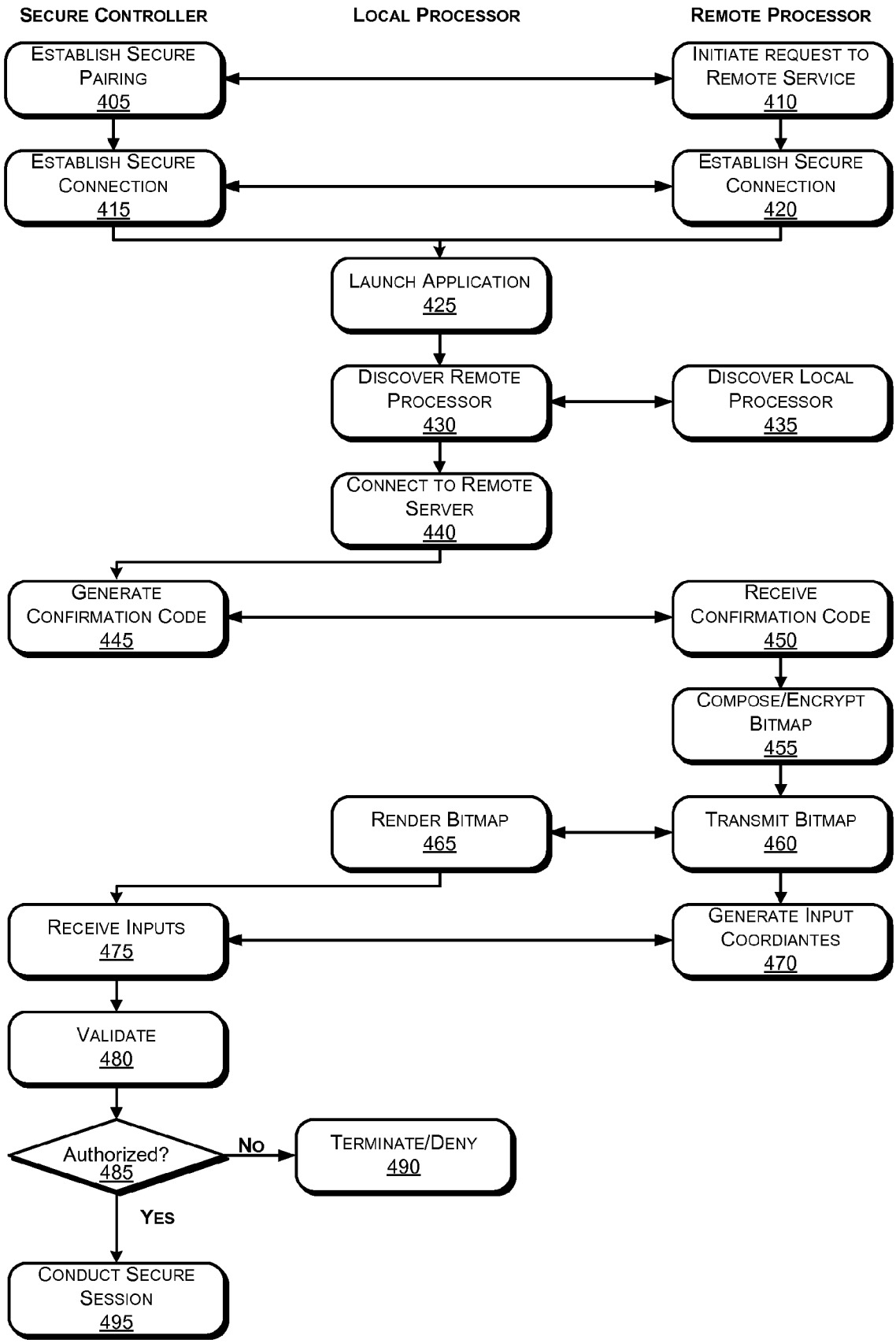
SECURE CONTROLLER
LOCAL PROCESSOR
REMOTE PROCESSOR
ESTABLISH SECURE PAIRING 405
INITIATE REQUEST TO REMOTE SERVICE 410
ESTABLISH SECURE CONNECTION 415
ESTABLISH SECURE CONNECTION 420
LAUNCH APPLICATION 425
DISCOVER REMOTE PROCESSOR 430
DISCOVER LOCAL PROCESSOR 435
CONNECT TO REMOTE SERVER 440
GENERATE CONFIRMATION CODE 445
RECEIVE CONFIRMATION CODE 450
COMPOSE/ENCRYPT BITMAP 455
RENDER BITMAP 465
TRANSMIT BITMAP 460
RECEIVE INPUTS 475
GENERATE INPUT COORDIANTES 470
VALIDATE 480
Authorized? 485
NO
TERMINATE/DENY 490
YES
CONDUCT SECURE SESSION 495

FIG. 4

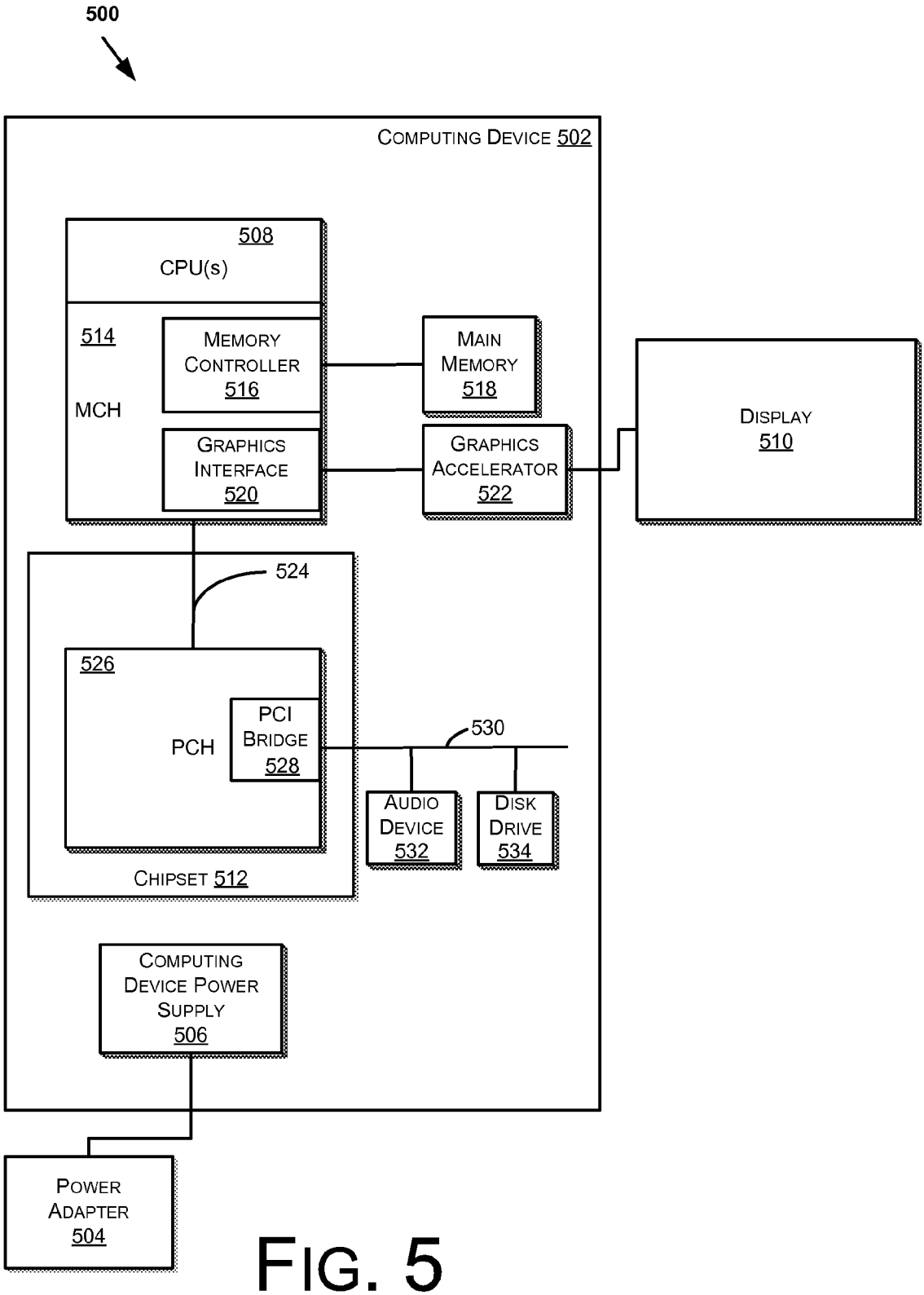
500
COMPUTING DEVICE 502
508
CPU(s)
514
MCH
MEMORY CONTROLLER 516
GRAPHICS INTERFACE 520
MAIN MEMORY 518
GRAPHICS ACCELERATOR 522
DISPLAY 510
524
526
PCH
PCI BRIDGE 528
530
AUDIO DEVICE 532
DISK DRIVE 534
CHIPSET 512
COMPUTING DEVICE POWER SUPPLY 506
POWER ADAPTER 504

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/033748

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/08(2009.01)i, H04W 12/06(2009.01)i, H04W 88/02(2009.01)i, H04W 92/18(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W 12/08; G06F 15/16; H04B 7/00; H04L 9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: relationship, network, authenticate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2006-0206932 A1 (FREDERICK C. CHONG) 14 September 2006 See paragraphs [0041]-[0063], claim 9 and figures 1b, 2.	1-22
A	US 2008-0307515 A1 (IGOR DROKOV et al.) 11 December 2008 See paragraphs [0083]-[0096], claim 1 and figures 1, 2.	1-22
A	US 2012-0079123 A1 (DAVID ANDREW BROWN et al.) 29 March 2012 See paragraphs [0029]-[0055], claims 1, 2 and figures 1-4.	1-22
A	US 2011-0078445 A1 (LU XIAO et al.) 31 March 2011 See paragraph [0027], claim 1 and figure 2.	1-22

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 DECEMBER 2012 (11.12.2012)	**12 DECEMBER 2012 (12.12.2012)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Yoo Sun Jung Telephone No. 82-42-481-5775

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/033748

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0206932 A1	14.09.2006	EP 1703694 A2	20.09.2006
		EP 1703694 A3	18.10.2006
		EP 1703694 B1	16.07.2008
		EP 1931107 A1	11.06.2008
		JP 05-021215 B2	22.06.2012
		JP 2006-260538 A	28.09.2006
		KR 10-2006-0100920 A	21.09.2006
		US 7900247 B2	01.03.2011
US 2008-0307515 A1	11.12.2008	EP 1802155 A1	27.06.2007
		EP 1969880 A1	17.09.2008
		EP 1969880 B1	30.05.2012
		WO 2007-072001 A1	28.06.2007
US 2012-0079123 A1	29.03.2012	EP 2434789 A1	28.03.2012
US 2011-0078445 A1	31.03.2011	None	